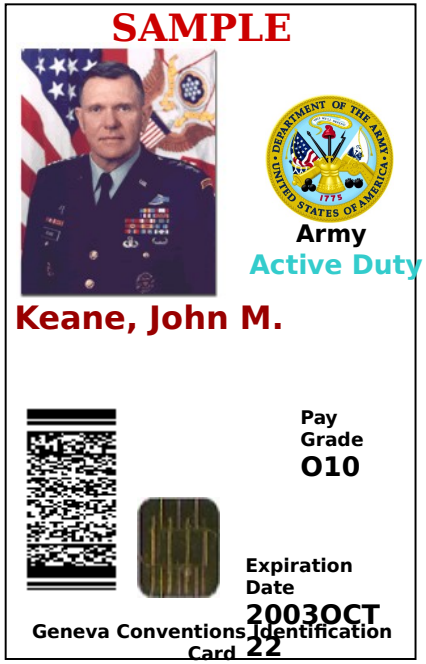
Common Access Card Update



Purpose

To provide an overview and information update of the Common Access Card (CAC).

Definitions

- **Common Access Card (CAC):** A mandated initiative that will use smart card technology to contain the following business applications; Personnel Identification, Building Access, and Network Access.
- **Smart Card (SC):** A credit card-sized device that can contain multiple technologies and individualized databases. The types of re-programmable and static technology normally found on a smart card include: an integrated chip, a magnetic stripe, and bar codes. The topology of the card can also contain printed information and images such as photos, text, and fingerprints.

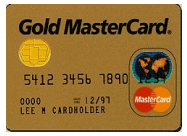
Definitions

- **Public-Key Infrastructure (PKI):** The people, policy, procedures, hardware/software, and facilities necessary to enable public key encryption, and digital signatures. Enhances information security and protects privacy.
- **Business Process Reengineering (BPR):** A structured analytical approach to examine core business processes and identify issues and improvement opportunities to remove non-value added activities, improve cycle-time, and lower process costs.
- **Functional Economic Analysis (FEA):** A structured proposal that includes an analysis of functional process needs or problems, proposed solutions, assumptions and constraints, alternatives, life-cycle costs, benefits and/or cost analysis, and investment risk analysis.

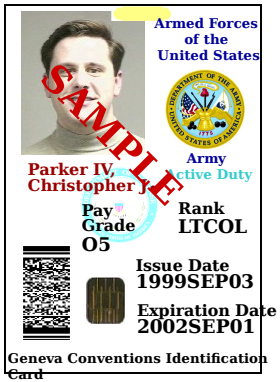
Common Access Card

A Credit Card-Sized Device That May Hold:

- Integrated Circuit Chip (IC)
- Magnetic Stripe
- Bar Codes
- Photo Identification
- Encryption and Authentication
- Biometrics
- Non-Contact Radio Frequency Transmitter



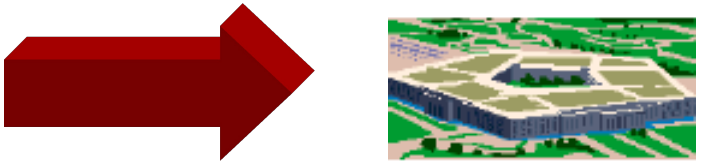
The CAC Provides...

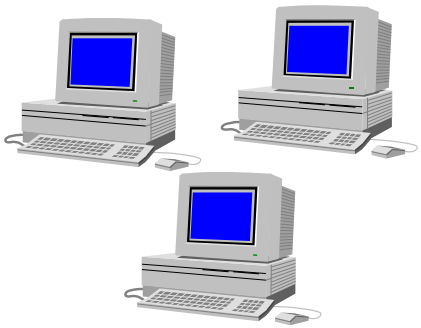


Personnel Identification

Replaces the “ID” Card

Building Access





Systems & Network Access

with PKI Application Provides:

- Digital Signature
- Data Encryption

Layout

Integrated Circuit Chip Location

- Army anticipates a 32K Chip.
- PKI Certificates will take 9.9K to 12.9K of the Chip.
- Future residual space (7K or greater) for other functional and service applications.

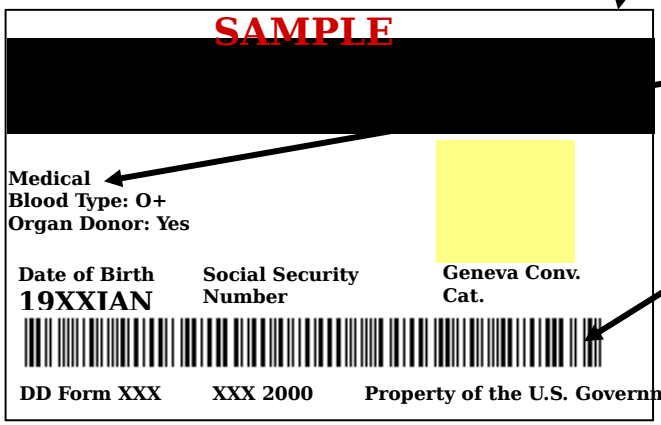
Barcode for Functional Applications

Current Uses Include:

- Army Food Management Information System (AFMIS) -- 3 sites
- USAREUR (Army/USAF) -- Motor Vehicle Registration -- 26 workstations
- USMC Flightline Access Control System -- 8 sites
- USAF Military Immunization Tracking System -- 26 workstations
- Little Creek Naval Station V00/B00

Magnetic Stripe

- Proposed use is for building and facility Access.



Medical Data

Shows the Blood Type and Organ Donor Status.

Barcode for Personnel Data

Where We Are Now

- **Policy Memorandums and Execution Plans state:**
  - **ID Card Sections will issue CACs *(DCSPER)***
  - **PKI maintenance conducted by DOIM *(DISC4)***
  - **Building access procedures *(DCSOPS)***
- **Beta Testing Phase I *(DRPO)***
  - **DOD operationally tests the CAC Software**
  - **Started at Fort Eustis 15 Feb 01**
  - **Heidelberg (28 Feb 01) / Korea (02 Mar 01)**
  - **Personnel identification functions**
- **Beta Testing Phase II *(DISC4/SET-D)***
  - **Test CAC-PKI applications**
  - **Ability/impact to operate in day to day environment**
  - **Start dates projected for Apr-Jun 01 at Fort Eustis, Heidelberg, Mannheim**
- **DRPO/ACO developing an implementation/fielding schedule**

Who Issues the CAC?

- DEERS/RAPIDS stations will be upgraded to issue the CACs with PKI certificates.
- There are approximately 305 DEERS/RAPIDS sites throughout all components of the Army.

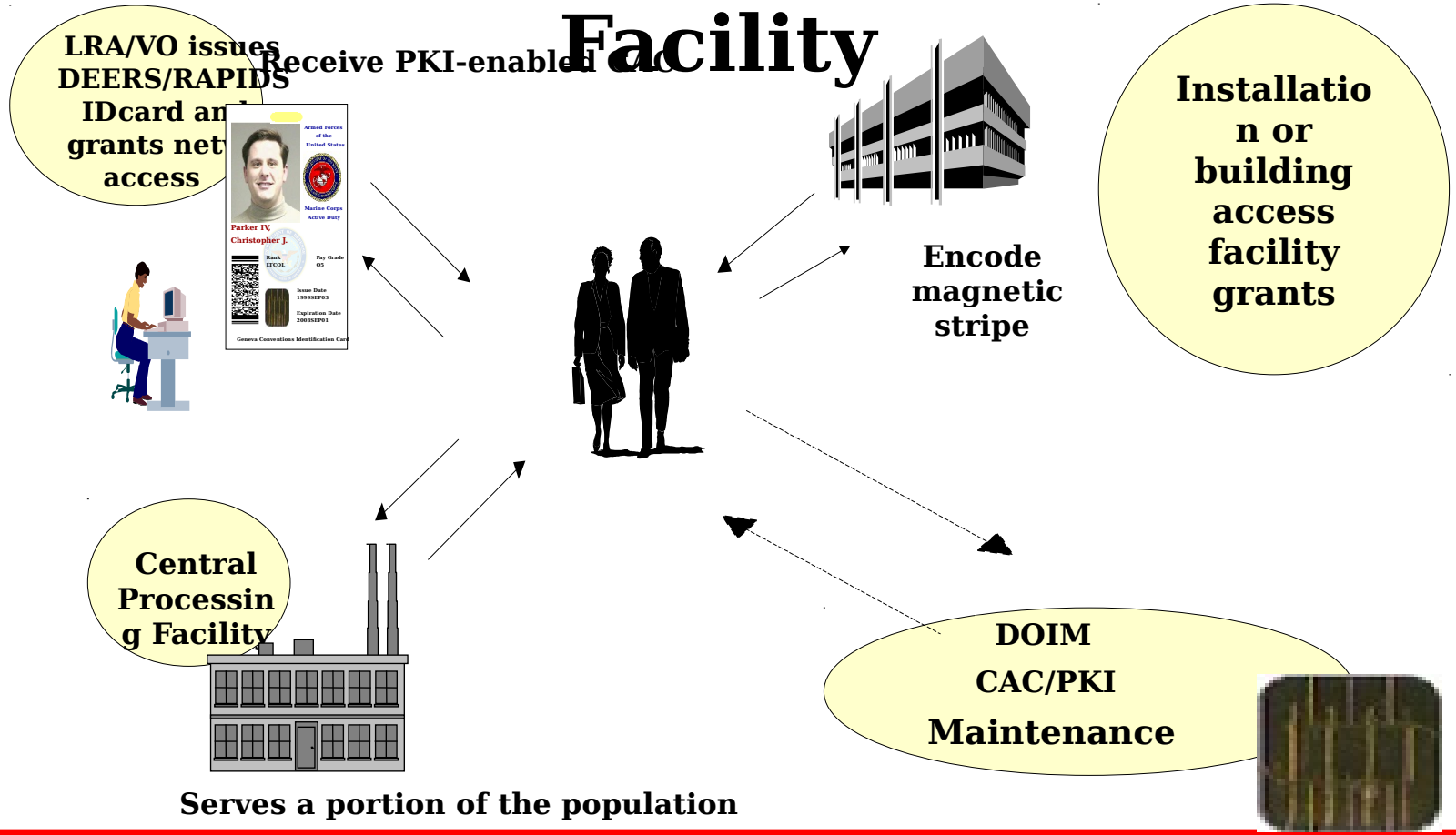
Who Performs PKI Maintenance?

Follow-on maintenance to the "chip" (i.e., changes to PKI certificates, email, PIN changes, PIN recovery, etc.) will be performed at a separate workstation by the DOIM or equivalent.

Minimizes workload on ID Card Section

CAC Issuance Process

Basic Implementation, Augmented Infrastructure, Central Processing Facility



CAC - "Key" to Personnel Redesign

Bottom Line

- **CAC's PKI token will be the "key" for secure access to personnel data and web-based applications**
- **Provides the means to electronically "sign" electronic transactions**
- **The CAC is an enabler, not just a data carrier/repository**
- **Supports transition to customer service in a virtual environment**

Summary

- CAC Beta Test
- Execution plans and policy documents to be finalized
- Implementation:
  - Define CPF
  - Card issuance with PKI certificates
  - DRPO/ACO developing fielding/training schedule
- Mandate for all Active Army soldiers, DOD civilians, selected Reserve Component soldiers, and selected contractors to have CAC by October 2002

For More Information

http://www.armyec.com

http://www.dmdc.osd.mil/smartcard